# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-154976
(43)Date of publication of application : 09.06.1998

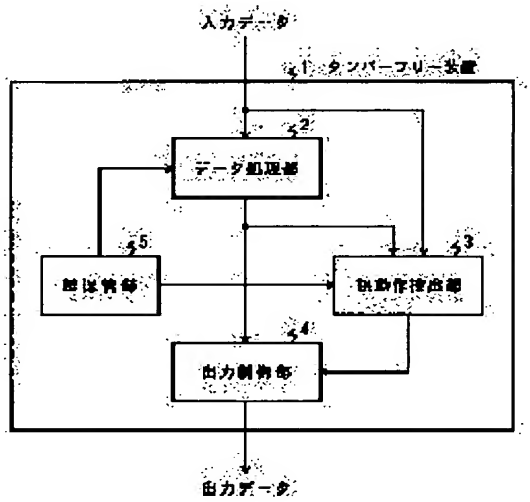
(51)Int.CI. H04L 9/10

(21)Application number : 08-311924
(22)Date of filing : 22.11.1996

(71)Applicant : TOSHIBA CORP
(72)Inventor : SHIMIZU HIDEO
SHINPO ATSUSHI
KAWAMURA SHINICHI

## (54) TAMPER-FREE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To protect the attack for estimating inside secret information by conducting a regulation to processing outputs when malfunction is detected in the prescribed data converting processing of outside input data, and applying a physical shock to an internal circuit from the outside to cause the malfunction, then observing the output thereof.
SOLUTION: A malfunction detecting part 3 detects whether or not a malfunction occurs in the ciphering processing of a data processing part 2 based on a plaintext and cipher data. When there is no malfunction, the cipher data is supplied from a control part 4. While if there is a malfunction, the output of cipher data is shut out by the control part 4. A person who tries to obtain secret information in a tamper-free apparatus enters processing target data and giving a physical shock such as heat and light or the like to the processing part 2, and tries to observe output data which reflects the effects of the malfunction depended on inside information. When the malfunction is caused by this shock in the processing part 2, since the detecting part 3 forbids output to the outside of the processed result which is reflected by the effect of the malfunction, the attacker is impossible to procure data, and impossible to obtain secret information in the apparatus 1.




LEGAL STATUS

[Date of request for examination] 11.09.2000
[Date of sending the examiner's decision of rejection] 08.01.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平10－154976**

(43)公開日　平成10年(1998)６月９日

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| Ｈ０４Ｌ　9/10 | | Ｈ０４Ｌ　9/00 | ６２１Ａ |
| | | | ６２１Ｚ |

審査請求　未請求　請求項の数11　ＯＬ　（全 15 頁）

(21)出願番号　特願平8－311924

(22)出願日　平成８年(1996)11月22日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　清水　秀夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　川村　信一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

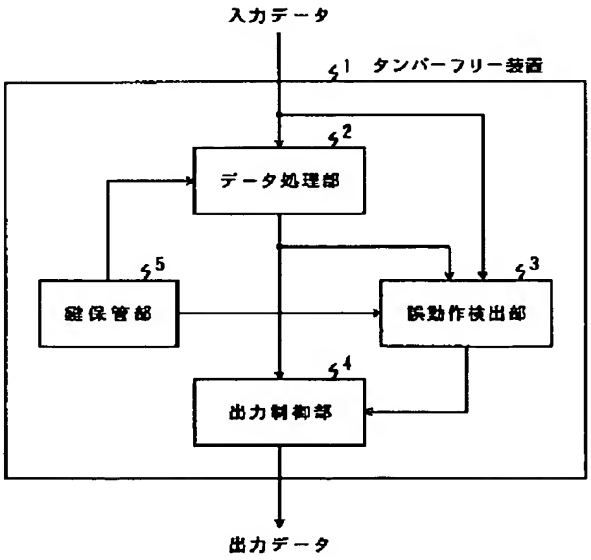
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　タンパーフリー装置

(57)【要約】

【課題】　外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を推測する攻撃法に対して防御可能なタンパーフリー装置を提供することを目的とする。

【解決手段】　内部に外部からの入力データに対して所定のデータ変換処理を施して出力するための手段を備え、内部情報への不正アクセスを防止するために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、前記データ変換処理の誤動作を検出する手段と、誤動作が検出された場合に前記処理の出力に所定の規制を施す出力規制手段とを備えたことを特徴とする。



1

【特許請求の範囲】

【請求項１】内部に外部からの入力データに対して所定のデータ変換処理を施して出力するための手段を備え、内部情報への不正アクセスを防止するために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、

前記データ変換処理の誤動作を検出する手段と、

誤動作が検出された場合に前記処理の出力に所定の規制を施す出力規制手段とを備えたことを特徴とするタンパーフリー装置。

【請求項２】入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、

入力データに対して鍵情報を用いた所定のデータ変換処理を施す手段と、

前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記所定のデータ変換処理において誤動作が発生したか否かを検出する手段と、

この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とするタンパーフリー装置。

【請求項３】入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、

予め定められた、鍵情報を用いて行う複数種類のデータ変換処理のうち実行すべきもの指示する情報を入力する手段と、

入力データに対して、指示されたデータ変換処理を施す手段と、

前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記データ変換処理において誤動作が発生したか否かを検出する手段と、

この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とするタンパーフリー装置。

【請求項４】入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、

予め定められた、複数の鍵情報のうち使用すべきもの指示する情報を入力する手段と、

2

入力データに対して、指示された前記鍵情報を用いた所定のデータ変換処理を施す手段と、

入力データに対して、指示されたデータ変換処理を施す手段と、

前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記データ変換処理において誤動作が発生したか否かを検出する手段と、

この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とするタンパーフリー装置。

【請求項５】前記検出する手段は、前記入力データに対して、前記所定のデータ変換処理と同一の処理を施し、得られた結果が前記所定のデータ変換処理により得られた結果と一致するか否かによって、誤動作が発生したか否かを検出することを特徴とする請求項１ないし４のいずれか１項に記載のタンパーフリー装置。

【請求項６】前記データ変換処理を施す手段における前記データ変換処理を行う回路と、前記検出する手段における前記処理を行う回路とを、同一半導体基板上で距離を離して設けたことを特徴とする請求項５に記載のタンパーフリー装置。

【請求項７】前記検出する手段は、前記データ変換処理の結果得られたデータに対して、前記所定のデータ変換処理の逆変換処理を施し、得られた結果が前記入力データと一致するか否かによって、誤動作が発生したか否かを検出することを特徴とする請求項１ないし４のいずれか１項に記載のタンパーフリー装置。

【請求項８】前記データ変換処理と前記逆変換処理とをパイプライン的に並列動作させるようにしたことを特徴とする請求項７に記載のタンパーフリー装置。

【請求項９】暗号アルゴリズムが積暗号である場合、各ラウンド処理毎に前記誤動作の検出を行うようにしたことを特徴とする請求項１ないし４のいずれか１項に記載のタンパーフリー装置。

【請求項１０】入力データに所定のデータ変換処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、

前記所定のデータ変換処理が準同型性を持つ場合、入力データに乱数を混入させたものに対して該データ変換処理を施し、得られた結果から、該乱数の影響を取り除いて、出力することを特徴とするタンパーフリー装置。

【請求項１１】前記所定のデータ変換処理は、暗号化処理、復号化処理、ディジタル署名、またはディジタル署名の署名検証であることを特徴とする請求項１ないし１０のいずれか１項に記載のタンパーフリー装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、放射線や他の物理手段により誤動作を生じさせ内部に封入された秘密を分解せずに暴こうとする攻撃に対して安全なタンパーフリー装置に関する。

【０００２】

【従来の技術】現在、コンピュータや記憶装置あるいは通信網など、情報を電子化して処理、保存、通信などする技術がかなり高度化されるとともに、ますます研究開発が盛んになってきている。また、このような技術は、実際に、様々な分野において様々な形で利用されている。中でも、情報を第３者から秘匿した状態で蓄積や転送などするための基盤技術である暗号技術の重要性は非常に高まっており、盛んに研究開発が行われているとともに、電子課金の情報、機密情報、著作権に係る情報あるいはプライバシーに関する情報などを扱うシステムに実際に利用されている。

【０００３】暗号技術を研究開発する場合、主に新たな暗号方式を提供するだけではなく、その新たな暗号方式における暗号解読の困難性を検証することも重要なテーマである。しかして、従来は、暗号解読は通信路の盗聴を前提としており、暗号化や復号を行う装置自体は、安全であって危険にさらされることはない、という前提があった。特に、例えばＩＣカードのように、分解や走査されることにより内部の情報を読み取ることを困難にしたタンパーフリー装置（タンパープルーフ装置あるいはタンパーレジスト装置とも呼ばれる）は、鍵の安全な保管装置としてだけではなく、計算能力（ＣＰＵ）も封入することで、鍵を外部に知られることなく、暗号化、復号化、認証処理などのデータ処理が可能な、安全なデータ処理装置を構成できるものと考えられていた。なお、タンパーフリー装置については、例えば、「“Ｓｕｐｅｒ ｄｉｓｔｒｉｂｕｔｉｏｎ：Ｔｈｅ Ｃｏｎｃｅｐｔ ｔｈｅ Ａｒｃｈｉｔｅｃｔｕｒｅ”、Ｍａｓａｊｉ Ｋａｗａｈａｒａ、ＴＨＥ ＴＲＡＮＳＡＣＴＩＯＮ ＯＦ ＴＨＥ ＩＥＩＣＥ、Ｖｏｌ．Ｅ７３、Ｎｏ．７、ＪＵＬＹ １９９０」に開示されている。

【０００４】ところが、ＢｒａｎｓｏｎやＬｉｎｄｓｔｒｏｍは、タンパーフリー装置を分解や操作することなく、内部の秘密情報を暴く新しい暗号解析技術を提示した（例えば、インターネットにおける“ｈｔｔｐ：／／ｗｗｗ．ｂｅｌｌｃｏｒｅ．ｃｏｍ／ＰＲＥＳＳ／ＡＤＶＳＲＹ９６／ｆａｃｔｓ．ｈｔｍｌ”）。その技術は、タンパーフリー装置に外部から放射線や電子、熱や振動など物理的な衝撃を加え、内部装置を誤動作（内部のレジスタが１ｂｉｔ反転する）させ、誤動作の結果得られた出力データを幾つか蓄積し、これら出力データに与えた誤動作の影響の仕方を観察することにより、内部情報を推測するというものである。このような技術は、これまでは想定されていなかったもので、ＩＣカードのようなタンパーフリーな暗号装置を利用者が手軽に利用できるようになったという社会背景と、暗号装置自身は攻撃されないことを前提としてきた従来の研究開発の指針とを考慮すると、既存の概念にある程度の転換を迫るものと言える。

【０００５】ＢｉｈａｍとＳｈａｍｉｒも同じ原理に基づいてＤＥＳのようなブロック暗号を解読する方法を提案した（例えば、インターネットにおける“ｈｔｔｐ：／／ｗｗｗ．ＣＳ．ｔｅｃｎｉｏｎ．ａｃ．ｉｌ／～ｂｉｈａｍ／ｄｆａ．ｈｔｍｌ”）。計算機によるシミュレーションの結果、この方法によれば、例えば約２００個程度の出力データの観察によりＤＥＳの５６ｂｉｔの鍵を手に入れることが可能であることが示されている。

【０００６】

【発明が解決しようとする課題】従来のタンパーフリー装置は、外部から放射線や電子、熱や振動などの物理的衝撃を加えることによって暗号化回路などの内部回路を誤動作させ、誤動作の反映された出力データを蓄積し観察することによって内部の秘密情報を推測する新しい暗号解読法に対して、対策が施されていないという問題があった。

【０００７】本発明は、上記事情を考慮してなされたもので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を推測する攻撃法に対して防御可能なタンパーフリー装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明（請求項１）は、内部に外部からの入力データに対して所定のデータ変換処理を施して出力するための手段を備え、内部情報への不正アクセスを防止するために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、前記データ変換処理の誤動作を検出する手段と、誤動作が検出された場合に前記処理の出力に所定の規制を施す出力規制手段とを備えたことを特徴とする。

【０００９】本発明によれば、タンパーフリー装置の内部回路が誤動作した場合、処理結果のデータ出力に所定の規制を施すので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【００１０】本発明（請求項２）は、入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、入力データに対して鍵情報を用いた所定のデータ変換処理を施す手段と、前記入力データおよび前記所定のデータ変換処理により得られたデータ

5

をもとにして、前記所定のデータ変換処理において誤動作が発生したか否かを検出する手段と、この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とする。

【００１１】本発明によれば、タンパーフリー装置の内部回路が誤動作した場合、処理結果をデータ出力しないので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【００１２】本発明（請求項３）は、入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、予め定められた、鍵情報を用いて行う複数種類のデータ変換処理のうち実行すべきもの指示する情報を入力する手段と、入力データに対して、指示されたデータ変換処理を施す手段と、前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記データ変換処理において誤動作が発生したか否かを検出する手段と、この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とする。

【００１３】本発明によれば、タンパーフリー装置の内部回路が誤動作した場合、処理結果をデータ出力しないので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【００１４】本発明（請求項４）は、入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、予め定められた、複数の鍵情報のうち使用すべきもの指示する情報を入力する手段と、入力データに対して、指示された前記鍵情報を用いた所定のデータ変換処理を施す手段と、入力データに対して、指示されたデータ変換処理を施す手段と、前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記データ変換処理において誤動作が発生したか否かを検出する手段と、この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とする。

【００１５】本発明によれば、タンパーフリー装置の内

6

部回路が誤動作した場合、処理結果をデータ出力しないので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【００１６】本発明（請求項５）は、請求項１ないし４のいずれか１項に記載のタンパーフリー装置において、前記検出する手段は、前記入力データに対して、前記所定のデータ変換処理と同一の処理を施し、得られた結果が前記所定のデータ変換処理により得られた結果と一致するか否かによって、誤動作が発生したか否かを検出することを特徴とする。

【００１７】本発明（請求項６）は、請求項５に記載のタンパーフリー装置において、前記データ変換処理を施す手段における前記データ変換処理を行う回路と、前記検出する手段における前記処理を行う回路とを、同一半導体基板上で距離を離して設けたことを特徴とする。

【００１８】本発明（請求項７）は、請求項１ないし４のいずれか１項に記載のタンパーフリー装置において、前記検出する手段は、前記データ変換処理の結果得られたデータに対して、前記所定のデータ変換処理の逆変換処理を施し、得られた結果が前記入力データと一致するか否かによって、誤動作が発生したか否かを検出することを特徴とする。

【００１９】本発明（請求項８）は、請求項７に記載のタンパーフリー装置において、前記データ変換処理と前記逆変換処理とをパイプライン的に並列動作させるようにしたことを特徴とする。

【００２０】これによって、誤動作検出処理に伴う処理時間の増大を防ぐことができる。本発明（請求項９）は、請求項１ないし４のいずれか１項に記載のタンパーフリー装置において、暗号アルゴリズムが積暗号である場合、各ラウンド処理毎に前記誤動作の検出を行うようにしたことを特徴とする。

【００２１】これによって、誤動作検出処理に伴う処理時間の増大を防ぐことができる。本発明（請求項１０）は、入力データに所定のデータ変換処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、前記所定のデータ変換処理が準同型性を持つ場合、入力データに乱数を混入させたものに対して該データ変換処理を施し、得られた結果から、該乱数の影響を取り除いて、出力することを特徴とする、本発明によれば、計算途中で生じた誤動作の影響を直接出力データに反映させないようにすることができるので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【００２２】本発明（請求項１１）は、請求項１ないし

１０のいずれか１項に記載のタンパーフリー装置において、前記所定のデータ変換処理は、暗号化処理、復号化処理、ディジタル署名、またはディジタル署名の署名検証であることを特徴とする。

【００２３】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。前述したように、例えばＩＣカードなどのようなタンパーフリー装置に、外部から放射線や電子、熱や振動など物理的な衝撃を加え、内部装置を誤動作させ、誤動作の結果得られた出力データを幾つか蓄積し、これら出力データに与えた誤動作の影響を観察することにより、装置内部に隠された秘密情報を暴こうとする新しい暗号解析技術が知られている。

【００２４】本実施形態は、概略的には、このような新たな攻撃方法に対処するために、タンパーフリー装置内で誤動作が生じた場合、内部情報の反映されたデータが外部に出力しないようにしたものである。

【００２５】図１に、本発明の第１の実施形態に係るタンパーフリー装置の構成を示す。このタンパーフリー装置１は、例えばその内部回路を半導体集積装置により形成し、これを樹脂で封止するなどの対策を講じることにより、（１）外部から内部回路中に存在するデータをアクセス不可とし、かつ（２）外部から内部回路の機能を変更させることを不可とする。すなわち、外部からは、処理に必要なデータを入力することと、処理結果のデータを得ることしかできないものとする。なお、タンパーフリー装置１の内部回路は、ハード・ワイヤードで形成しても良いし、再書き込み不能のＲＯＭ回路に書き込んだプログラムをＣＰＵで実行するような構成で形成しても良い。

【００２６】図示はしていないが、タンパーフリー装置１の電源は、外部から供給するようにしても良いし、電池を内蔵しても良い。また、タンパーフリー装置１は、必要に応じて外部装置とのインターフェース手段を備えても良い。また、タンパーフリー装置１を外部装置に接続する端子には、種々のコネクタ類が使用可能である。なお、タンパーフリー装置１に無線通信手段を内蔵し、無線により接続しても良い。

【００２７】さて、図１に示すように、このタンパーフリー装置１は、データ処理部２、誤動作検出部３、出力制御部４、鍵保管部５を備えている。データ処理部２は、共通鍵、または暗号鍵もしくは復号鍵などの鍵情報を用いたデータ変換を伴う所定のデータ処理を行う。所定のデータ処理としては、例えば、ＤＥＳやＦＥＡＬなどの共通鍵暗号方式あるいはＲＳＡなどの公開鍵暗号方式等に基づいた、暗号化、復号化、ディジタル署名などの認証データ生成、ディジタル署名の署名検証などの認証データ検証などがある。ここでは、データ処理部２の処理内容はあらかじめ定められた１つのものであるとする。

【００２８】より具体的な構成としては、このデータ処理部の処理内容が暗号化の場合、データ処理部は暗号化部などとなる。また、データ処理部の処理内容が復号化、認証データ生成あるいは認証データ検証などの場合も、それぞれ同様に、復号化処理部、認証データ生成部もしくは署名部、認証データ検証部もしくは検証部などとなる。

【００２９】誤動作検出部３は、データ処理部２に対する入力データと、データ処理部２による処理結果のデータと、所定の鍵情報とをもとに、データ処理部２に誤動作が生じたか否かを判断し、判断結果に応じて所定の制御信号を出力する。

【００３０】誤動作検出部３で用いる鍵情報は、データ処理部２で用いる鍵情報に対応するものであり、データ処理部２の処理で用いる暗号方式やこの誤動作検出部３で用いる誤動作検出方式に応じて定まる。

【００３１】誤動作検出方式としては、詳しくは後述するが、（１）データ処理部２と同一の処理を同一入力データに対して施し、得られた２つの処理結果が一致するか否か比較する（一致しなかった場合に誤動作発生と判断する）もの、（２）データ処理部２の処理結果に対して逆変換処理を施し、この結果ともとの入力データが一致するか否か比較する（一致しなかった場合に誤動作発生と判断する）ものなど、種々の方法が考えられる。

【００３２】鍵保管部５は、データ処理部２にて用いる鍵情報と誤動作検出部３で用いる鍵情報を保管している。なお、鍵保管部５に、誤動作検出部３で用いるために、暗号化情報を受け渡しする相手側装置の秘密鍵が保管されている場合、この相手側装置の秘密鍵は、誤動作検出部３以外からはアクセスできないものとする。

【００３３】出力制御部４は、誤動作検出部３によりデータ処理部２に誤動作が発生しなかったと判断された場合、データ処理部２の処理結果を外部に出力し、誤動作検出部３によりデータ処理部２に誤動作が発生したと判断された場合、データ処理部２の処理結果を外部に出力しないようにする。

【００３４】この出力制御の方法としては、（１）誤動作検出部３は、誤動作を検出したときのみ誤動作検出信号を出力し、出力制御部４は、誤動作検出部３から誤動作検出信号が渡されたときのみ、処理結果を外部に出力せず、それ以外の場合は処理結果を出力する方法、

（２）誤動作検出部３は、誤動作を検出しなかったときのみ正常動作検出信号を出力し、出力制御部４は、誤動作検出部３から正常動作検出信号が渡されたときのみ、処理結果を外部に出力し、それ以外の場合は出力しない方法、（３）誤動作検出部３は、誤動作を検出しなかったとき正常動作検出信号を出力し、誤動作を検出したとき誤動作検出信号を出力し、出力制御部４は、誤動作検出部３から正常動作検出信号が渡されたときのみ、処理結果を外部に出力し、誤動作検出部３から誤動作検出信

号が渡されたときのみ、処理結果を外部に出力せず、何らかの理由でどちらの信号も渡されなかった場合、エラー処理（例えば、エラー回数が一定値になるまでは誤動作検出信号が与えられたものとみなし、エラー回数が一定値を越えたら当該タンパーフリー装置の機能自体を停止させるなど）を行う方法など、種々の方法が考えられる。

【００３５】図２に、本実施形態に係るタンパーフリー装置の動作の流れを示す。処理対象となるデータ（例えばメッセージ）が入力されると、鍵保管部５に格納された鍵を使って、データ処理部２によりデータ変換処理がなされる（ステップＳ１）。

【００３６】次に、誤動作検出部３は、データ処理部２の誤動作の有無を検出する（ステップＳ２）。データ処理部２の処理に誤動作はなかったと判断された場合（ステップＳ３）、処理結果は出力制御部４を介して外部に出力される（ステップＳ４）。

【００３７】一方、データ処理部２の処理に誤動作が生じたと判断された場合（ステップＳ３）、処理結果は出力制御部４にて遮断され、外部への出力が禁止される（ステップＳ５）。

【００３８】また、例えばデータ処理部２の機能が暗号化である場合には、タンパーフリー装置のより具体的な動作の流れは次のようになる。なお、復号化、認証データ生成あるいは認証データ検証などの場合も、それぞれ同様である。

【００３９】暗号化対象となる平文メッセージなどのデータが入力されると、データ処理部（この場合、暗号部に相当）２は、鍵保管部５に格納された暗号鍵（もしくは共通鍵）を使って、このメッセージを暗号化する（ステップＳ１）。

【００４０】次に、誤動作検出部３は、データ処理部２の暗号化処理に誤動作が発生したか否かを、平文データと暗号化データをもとにして検出する（ステップＳ２）。例えば、平文データの暗号化を再度実行して、両方の暗号化データが一致するか否かを調べる。あるいは、暗号化データを復号してもとの平文データに戻るか否かを調べる。

【００４１】データ処理部２の暗号化処理に誤動作はなかったと判断された場合（ステップＳ３）、暗号化データは出力制御部４を介して外部に出力される（ステップＳ４）。

【００４２】一方、データ処理部２の暗号化処理に誤動作が生じたと判断された場合（ステップＳ３）、暗号化データは出力制御部４にて遮断され、外部への出力が禁止される（ステップＳ５）。

【００４３】さて、前述したような新しい暗号解析技術を用いて、タンパーフリー装置１の内部に隠された鍵情報などの秘密情報を暴こうとする者は、処理対象のデータを入力し、そしてデータ処理部３を誤動作させるために装置本体に放射線や電子パルス、磁気、熱、光等を当て、内部情報に依存した誤動作の影響が反映された出力データを観測しようとする。

【００４４】しかしながら、本実施形態によれば、タンパーフリー装置１に放射線等が当てられデータ処理部３に誤動作が生じた場合、誤動作検出部３の働きにより、誤動作の影響を反映した処理結果が外部に出力されることが禁止される。この結果、攻撃者は、誤動作が生じた場合の出力データを得ることはできず、タンパーフリー装置１内部の秘密情報を暴くことはできない。

【００４５】このように、本実施形態に係るタンパーフリー装置１は、タンパーフリー装置自体に物理的衝撃を与え誤動作を起こさせて暗号解読しようとする新しい暗号解析技術に対し、簡易な構成で確実に対抗できる点で、非常に優れたものとなっている。

【００４６】以下では、図１で説明した構成を発展させたものやより具体化したものなどについて幾つかの例を示す。図３は、図１の構成において、誤動作検出部３による検出結果を示す制御情報を外部に出力するようにしたものである。この場合、制御情報の出し方には幾つかのものが考えられる。

【００４７】例えば、誤動作検出部３は、誤動作がなかったと判断された場合にのみ、誤動作がないことを示す信号を出力するようにしても良い。あるいは、誤動作があったと判断された場合にのみ、誤動作があったことを示す信号を出力するようにしても良い。あるいは、誤動作がなかったと判断された場合に、誤動作がないことを示す信号を出力し、誤動作があったと判断された場合に、誤動作があったことを示す信号を出力するようにしても良い。

【００４８】図４は、図１の構成において、鍵保管部５に複数の鍵をＩＤ番号と対応付けて格納しておき、データ処理部２の処理で用いる鍵を外部から指定可能にしたものである。なお、データ処理部２で用いる鍵と、誤動作検出部３で用いる鍵が異なる場合、例えば、データ処理部２で暗号鍵を用いて暗号化し、誤動作検出部３でこの暗号鍵とは異なる復号鍵を用いて復号化するような場合、両方の鍵を対応付けて格納しておく。

【００４９】このようにした場合、処理対象となるデータの入力の前もしくは同時もしくは後に、使用する鍵のＩＤ番号を指示入力する。データ処理部２や誤動作検出部３は、指示されたＩＤ番号に対応する鍵を用いて処理を行う。

【００５０】図５は、図１の構成において、データ処理２が複数の種類のデータ処理を実行可能とし、データ処理部２の処理内容の種類を外部から指定可能にしたものである。

【００５１】データ処理内容の組み合わせは任意であるが、具体例としては次のようなものがある。

（１）幾つかの異なる方式の暗号化機能を備えるケース

（２）幾つかの異なる方式の復号化機能を備えるケース
（３）幾つかの異なる方式の認証データ生成機能を備えるケース
（４）幾つかの異なる方式の認証データ検証機能を備えるケース
（５）１または複数の対の暗号化機能と復号化機能を備えるケース
（６）１または複数の対の認証データ生成機能と認証データ検証機能を備えるケース
（７）１または複数の対の暗号化機能と復号化機能、および１または複数の対の認証データ生成機能と認証データ検証機能を備えるケース
なお、処理に応じて異なる鍵を用いることがある場合、処理のＩＤ番号とその処理で使用する鍵とを対応付けて鍵保管部５に格納しておく。

【００５２】図６に、図５のように構成したタンパーフリー装置の動作の流れを示す。まず、実行すべきデータ処理の内容を示すＩＤ番号を入力する（ステップＳ２１）。

【００５３】例えばデータ処理部２の機能が暗号化または復号化であり、暗号化処理を指示する場合には、暗号化処理のＩＤ番号を入力する（ステップＳ２１）。ステップＳ２１の入力の前もしくは同時もしくは後に処理対象となるデータ（例えばメッセージ）が入力されると、鍵保管部５に格納された鍵を使って、データ処理部２によりデータ変換処理がなされる（ステップＳ２２）。

【００５４】次に、誤動作検出部３は、データ処理部２の誤動作の有無を検出する（ステップＳ２３）。データ処理部２の処理に誤動作はなかったと判断された場合（ステップＳ２４）、処理結果は出力制御部４を介して外部に出力される（ステップＳ２５）。

【００５５】一方、データ処理部２の処理に誤動作が生じたと判断された場合（ステップＳ２４）、処理結果は出力制御部４にて遮断され、外部への出力が禁止される（ステップＳ２６）。

【００５６】なお、図３で説明した誤動作検出部５が検出結果を示す制御情報を外部に出力する構成、図４で説明した外部から鍵の指定を可能とする構成、図５で説明した外部から処理内容の指定を可能とする構成は、任意に組み合わせることが可能である。

【００５７】例えば、図４と図５を組み合わせて、外部から鍵の指定を可能とするとともに、処理内容の指定を可能とする場合、鍵保管部５に複数の鍵（または暗号鍵と復号鍵の対）を鍵ＩＤ（または鍵ＩＤおよび処理ＩＤ）と対応付けて格納しておき、処理対象となるデータの入力の前もしくは同時もしくは後に、処理ＩＤと鍵ＩＤを指示入力するようにすればよい。

【００５８】以下では、誤動作検出部３のより具体的な例について説明する。前述したように誤動作検出方式としては、主として、（１）データ処理部２と同一の処理を同一入力データに対して施し、得られた２つの処理結果が一致するか否か比較する（一致しなかった場合に誤動作発生と判断する）もの、（２）データ処理部２の処理結果に対して逆変換処理を施し、この結果ともとの入力データが一致するか否か比較する（一致しなかった場合に誤動作発生と判断する）ものが考えられる。

【００５９】ここで、説明の便宜上、（１）の方法を２重化法、（２）の方法を検算法と呼ぶ。データ処理部２の処理内容にかかわらず２重化法は常に適用可能であるが、検算法はデータ処理部２の処理内容に依存して適用可能な場合と適用不可の場合がある。

【００６０】データ処理部２の処理内容として検算法が適用可能なものは、例えば以下のような処理である。
（ａ）ある処理とその逆変換処理で同一の鍵を用いるもの
（ｂ）公開鍵暗号方式に基づく可逆な処理で、検算処理に相手側の秘密鍵が不要なもの
（ｃ）公開鍵暗号方式に基づく可逆な処理でかつ検算処理に相手側の秘密鍵を必要とするものであって、相手側の秘密鍵が当該誤動作検出のために使用可能な場合
なお、データ処理部２の処理が不可逆の処理（例えばＤＳＡ）である場合、検算法を適用することはできない。

【００６１】（ａ）の具体例としては、共通鍵暗号方式に基づく暗号化と復号化（例えばＤＥＳ、ＦＥＡＬ）が該当する。
（ｂ）の具体例としては、公開鍵暗号方式に基づく復号化、公開鍵暗号方式に基づく認証データ生成で可逆なもの（例えばＲＳＡ）が該当する。

【００６２】（ｃ）の具体例としては、公開鍵暗号方式に基づく暗号化、公開鍵暗号方式に基づく認証データ検証で可逆なもの（例えばＲＳＡ）が該当する。
図７に、図１～図６を用いて説明したタンパーフリー装置の誤動作検出部３の構成に２重化法を用いた場合の一例を示す。

【００６３】データ処理部３１は、データ処理部２と同一の処理機能を持つものである。比較部３２は、データ処理部２の出力とデータ処理部３１の出力を比較し、前述したように比較結果に応じて所定の制御信号を出力する。

【００６４】ここで、データ処理部２とデータ処理部３１とは、回路を独立させて、互いの処理を同時実行可能にすれば、誤動作検出処理に要する時間を大幅に削減することができる。

【００６５】なお、誤動作検出処理に要する時間が多少かかっても、回路量を削減したい場合には、データ処理部２とデータ処理部３１を１つの回路で共用するように構成してもよい。

【００６６】図８に、図１～図６を用いて説明したタンパーフリー装置の誤動作検出部３の構成に検算法を用いた場合の一例を示す。逆変換部３３は、データ処理部２

で行う処理に対する逆変換処理の機能を持つものである。比較部３２は、データ処理部２の出力と逆変換部３３の出力を比較し、前述したように比較結果に応じて所定の制御信号を出力する。

【００６７】ここで、誤動作検出処理による全体の処理性能の低下を防ぐために、暗号化処理と誤動作検出処理を並列化してもよい。例えば、データ処理部２と逆変換部３３とで回路を独立させ、これにパイプライン処理を適用すれば、誤動作検出処理に要する時間を大幅に削減することができる。

【００６８】例えば図９に示すように、データ処理部２で暗号化を行い、逆変換部３３で復号化を行う場合、入力ブロック＃１は、暗号化された後、誤動作検出（検算）のために復号される。一方、このブロック＃１の復号が行われている間、次のブロック＃２の暗号化が行われる。これによって、１つのブロックが入力されてから出力が得られるまで２単位時間の遅延がかかるだけで、誤動作検出処理を行わない場合と略同様の処理性能を得ることができる。

【００６９】なお、データ処理部２と逆変換部３３の構成が同一になる場合には、誤動作検出処理に要する時間が多少かかっても、回路量を削減したいならば、データ処理部２と逆変換部３３を１つの回路で共用するように構成してもよい。

【００７０】以下では、図１～図６を用いて説明したタンパーフリー装置のデータ処理部２の処理がラウンド関数を用いる場合の構成例について説明する。ＤＥＳやＦＥＡＬのようなラウンド関数を用いる暗号アルゴリズムでは、暗号化したい平文に対し、鍵をパラメータとするラウンド関数を繰り返し適用する。例えば、４段の変換を用いる場合、まず平文は第１のラウンド関数により変換され、変換結果は第２のラウンド関数により変換され、この変換結果がさらに第３のラウンド関数と第４のラウンド関数により順次変換される。暗号アルゴリズムによって、ラウンド関数の段階数が定められる。復号化についても同様である。

【００７１】ところで、このようなラウンド関数を積み重ねた積暗号方式では、各ラウンド毎に誤動作検出を行うことが可能である。そこで、例えば暗号化の場合、もともとの暗号化回路の他に、誤動作検出のための暗号化回路（２重化法の場合）あるいは復号化回路（検算法の場合）を独立して持ち、並列演算を行うことにより、誤動作検出処理による全体の処理速度の増大を防ぐことが可能となる。つまり、あるラウンド関数の処理結果をもとに誤動作検出処理を実行するのと同時に後続するラウンド関数の暗号化処理（あるいは復号化処理）を行うことができる。そして、あるラウンド関数の処理に誤動作が生じたと判断された場合、その時点で処理を停止させ、あるいは最終的な処理結果が外部に出力されるのを禁止させることができる。

【００７２】図１０に、ラウンド数が４段で、かつ誤動作検出部３の構成に２重化法を用いた場合の一例を示す。暗号化回路２０１～２０４，３０１～３０４は、それぞれラウンド関数に対応する。

【００７３】比較部３１１～３１４では、２つの暗号化されたデータを比較し、その結果を動作制御部３２１に通知する。動作制御部３２１は、比較部３１１～３１３から誤動作検出の通知を受けた場合、次段以降の処理を停止させ、最終段の比較部３１４から誤動作検出の通知を受けた場合、出力制御部４を制御して最終的な処理結果が外部に出力されないようにする。

【００７４】なお、復号化を行う場合も、同様の構成である。図１１に、ラウンド数が４段で、かつ誤動作検出部３の構成に検算法を用いた場合の一例を示す。

【００７５】暗号化回路２０１～２０４は、それぞれラウンド関数に対応する。復号化回路３３１～３３４は、それぞれ対応する暗号化回路２０１～２０４の逆関数を実行する。

【００７６】比較部３１１～３１４では、対応する暗号化回路２０１～２０４への入力データと、対応する復号化回路３３１～３３４の処理結果を比較し、その結果を動作制御部３２１に通知する。

【００７７】動作制御部３２１は、比較部３１１～３１３から誤動作検出の通知を受けた場合、次段以降の処理を停止させ、最終段の比較部３１４から誤動作検出の通知を受けた場合、出力制御部４を制御して最終的な処理結果が外部に出力されないようにする。

【００７８】なお、復号化を行う場合も、同様の構成である。図１２に、図１０と図１１のタンパーフリー装置の処理の流れを示す。まず、データ処理部２における第１段のラウンド関数を実行する（ステップＳ３１）。なお、図１０の構成の場合、誤動作検出部３における第１段のラウンド関数を同時に実行できる。

【００７９】次に、データ処理部２における第２段のラウンド関数を実行するとともに（ステップＳ３２）、第１段のラウンド関数の実行についての誤動作検出処理を行う（ステップＳ３３）。なお、図１１の構成の場合、誤動作検出部３における第１段のラウンド関数を実行した後に、比較部３１１での比較処理を行う。

【００８０】誤動作が検出された場合（ステップＳ３４）、ラウンド関数の実行を停止させる処理が実行される（ステップＳ３５）。誤動作が検出されなかった場合（ステップＳ３４）、そのままラウンド関数の実行は継続される。

【００８１】以降、このような動作が最終段（ここでは４段目）まで繰り返される（ステップＳ３６～Ｓ４３）。そして、最終段の誤動作検出処理が実行され（ステップＳ４４）、誤動作が検出された場合（ステップＳ４５）、最終的な処理結果の外部への出力は禁止され（ステップＳ４６）、誤動作が検出されなかった場合

（ステップＳ４５）、最終的な処理結果が外部へ出力される（ステップＳ４７）。

【００８２】なお、図１０～図１２では、ラウンド数が４段である場合について説明したが、もちろん、本構成は、所望のラウンド数のものに適用可能である。ところで、図１０や図１１の構成において、ラウンド対応部分を１組の回路で共用し、回路量を削減することも可能である。

【００８３】そのような構成の一例として、図１３に、データ処理部２と誤動作検出部３の両方で暗号化を行う場合の構成例を示す。また、図１４に、データ処理部２で暗号化を行い、誤動作検出部３で復号化を行う場合の構成例を示す。伝える。

【００８４】選択回路２１１は、外部からのデータ入力時には、入力データを暗号部２０１側に伝え、その他ではラウンド関数の実行のために、選択回路２１２の出力を伝える。

【００８５】選択回路２１２は、最終段のラウンド関数の実行までは、暗号部２０１の出力を選択回路２１１に伝え、最終段のラウンド関数の実行結果は、出力制御部４に伝える。

【００８６】以下では、これまで説明してきた各実施形態の変形例を幾つか示す。各実施形態では、誤動作を検出したら外部への出力を禁止するものであったが、その代わりに、誤動作を検出したら、再度計算を繰り返すようにしても良い。また、この場合に、その繰り返しが一定数を越えたら、装置自体を所定の方法でロックして使用できなくするようにしても良い。あるいは、繰り返しが一定数を越えた場合に、その旨を示す信号を外部に出力するようにしても良い。

【００８７】また、誤動作を検出したら、外部にデータを出力しない代わりに、乱数を出力するようにしても良い。この場合、出力データを全て乱数に置き換えても良いし、装置内部の秘密情報の反映を解消できる程度で、出力データの一部のみ乱数に置き換えても良い。

【００８８】また、ＲＳＡ暗号方式を用いる場合、パラメータｅを小さくすることにより、復号化に対する検算（暗号化）時間を短くしても良い。ところで、前述した暗号化回路などのデータ処理部を２重化することにより誤動作を検出する方式において、同じ役割を果たす２重化された２つの回路の配線が互いに隣り合わず、物理的に離れているようなレイアウトに配置すると好ましい。

【００８９】例えば、図１５では、半導体基板３４０上で、第１の暗号化回路３４１と、第２の暗号化回路３４３とを、比較回路３４２を挟んで、物理的に距離をあけて配置させた様子を示している。

【００９０】暗号解読のために誤動作を起こさせようとタンパーフリー装置自体に外部より物理的衝撃を加える際に、放射線を焦点を絞って照射することが困難であるなど、物理現象をスポット的に生じさせることが困難である場合、上記のようにすることで、２重化された２つの回路で誤動作の生じる箇所を互いに異ならせるようにし、偶然に２つの回路で同一の誤動作が発生し、比較回路で誤動作が見過ごされるようなことをほぼ完全に回避することができる。

【００９１】以上では、タンパーフリー装置内で、１種類の処理を施す例を示してきたが、複数の処理、例えば、暗号化と電子署名の２つの処理（あるいは復号化と電子署名検証）を連続して行うようにしても良い。その際、複数の処理の少なくとも１つに誤動作が検出された場合、すべての処理について外部へのデータ出力を禁止する方法や、誤動作が検出された処理についてのみ外部へのデータ出力を禁止する方法などが考えられる。

【００９２】次に、本発明の第２の実施形態に係るタンパーフリー装置について説明する。これまで説明してきた第１の実施形態は、概略的には、処理にあたっての誤動作を検出したら処理結果の出力を禁止するものであった。

【００９３】この第２の実施形態は、誤動作の有無は判断せず、処理結果も常に出力することとし、その代わりに、誤動作の結果得られる出力データに内部状態が反映されないように工夫したものである。

【００９４】図１６に、本実施形態にかかるタンパーフリー装置の内部機能の一例を示す。４０１は、この処理におけるもともとの変換Ｅを実行するデータ処理部である。例えば、変換Ｅは、暗号化あるいは復号化に該当する。

【００９５】４０２は、変換Ｅの逆変換$E^{-1}$を実行する逆変換部である。４０３と４０６は、同一の所定の演算を行う演算部である。この所定の演算を示す演算子を記号○で表すこととする。

【００９６】４０４は、所定の方法で乱数Ｒを発生する乱数発生部である。４０５は、乱数Ｒの逆元$R^{-1}$を求める逆元処理部である。なお、４０４と４０５を一体化させて、乱数Ｒとその逆元$R^{-1}$を同時に求めても良い。

【００９７】ここでは、排他的論理和など所定の演算子○に対して、Ｅ（Ａ○Ｂ）＝Ｅ（Ａ）○Ｅ（Ｂ）が成立する準同型性を持つ暗号化関数を使用する暗号（例えばＲＳＡ暗号）を考える。

【００９８】なお、Ｃ○ａ＝Ｃとなる場合に、Ｄに対して、$D○D^{-1}=a$とする$D^{-1}$を、Ｒの逆元と呼び、Ｒの逆元$R^{-1}$を求める処理を、逆元処理と呼ぶ。例えば、演算子○が排他的論理和を表す場合、ａ＝１であり、演算子○が排他的論理積を表す場合、ａ＝０である。

【００９９】さて、準同型性を持つ暗号化関数を使用する暗号では、乱数Ｒを逆変換$E^{-1}$した結果$E^{-1}$（Ｒ）を求め、暗号化対象となる平文Ｍと$E^{-1}$（Ｒ）に演算○を施した結果$M○E^{-1}$（Ｒ）を求め、この$M○E^{-1}$（Ｒ）を変換Ｅした結果Ｅ（$M○E^{-1}$（Ｒ））を求め、また、上記の乱数Ｒの逆元$R^{-1}$を求め、Ｅ（$M○E^{-1}$（Ｒ））

とR$^{-1}$に演算○を施した結果E（M）○E（E$^{-1}$（R））○R$^{-1}$を求めると、これが平文Mを変換Eした結果E（M）に等しいという性質がある。

【０１００】すなわち、E（M○E$^{-1}$（R））○R$^{-1}$
＝E（M）○E（E$^{-1}$（R））○R$^{-1}$
＝E（M）○R○R$^{-1}$
＝E（M）
となる。

【０１０１】本実施形態では、このような演算過程で乱数を混入させるという操作を行ったにもかかわらず結果は乱数に依存せずに一定であるという性質を利用している。すなわち、変換Eの処理中に発生した誤動作の影響は、乱数Rを混入させることにより拡散され、暗号解読に役立つ情報を得ることができなくなる。この操作は、物理的手段により誤動作を誘発させて暗号を解読しようとする新たな攻撃法に対して絶大な効果がある。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１０２】

【発明の効果】本発明によれば、タンパーフリー装置の内部回路が誤動作した場合、処理結果をデータ出力しないので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態にかかるタンパーフリー装置の一構成例を示す図

【図２】同実施形態に係るタンパーフリー装置の動作の流れの一例を示すフローチャート

【図３】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図４】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図５】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図６】同実施形態に係るタンパーフリー装置の動作の流れの他の例を示すフローチャート

【図７】誤動作検出部の一例を示す図

【図８】誤動作検出部の他の例を示す図

【図９】パイプライン処理による高速化を説明するための図

【図１０】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図１１】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図１２】同実施形態に係るタンパーフリー装置の動作の流れの他の例を示すフローチャート

【図１３】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図１４】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

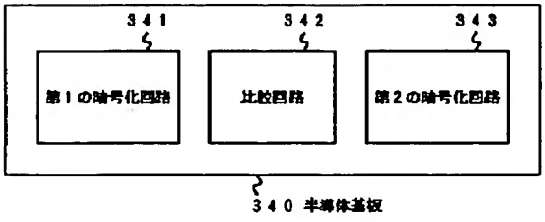
【図１５】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図１６】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

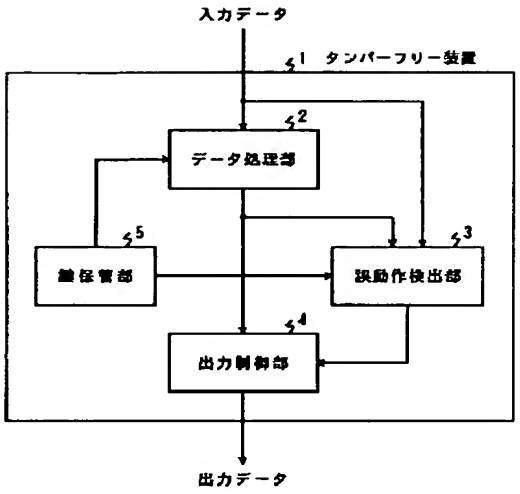
【符号の説明】

１…タンパーフリー装置
２，４０１…データ処理部
３…誤動作検出部
４…出力制御部
５…鍵保管部
３１…データ処理部
３２…比較部
３３，４０２…逆変換部
２０１～２０４，３０１～３０４…暗号化回路
３１１～３１４…比較部
３２１…動作制御部
３３１～３３４…復号化回路
２１１，２１２…選択回路
４０３，４０６…演算部
４０４…乱数発生部
４０５…逆元処理部

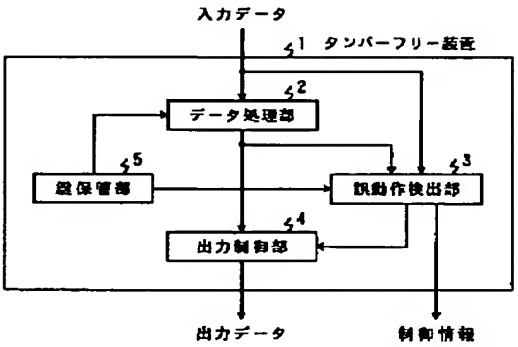
【図１５】



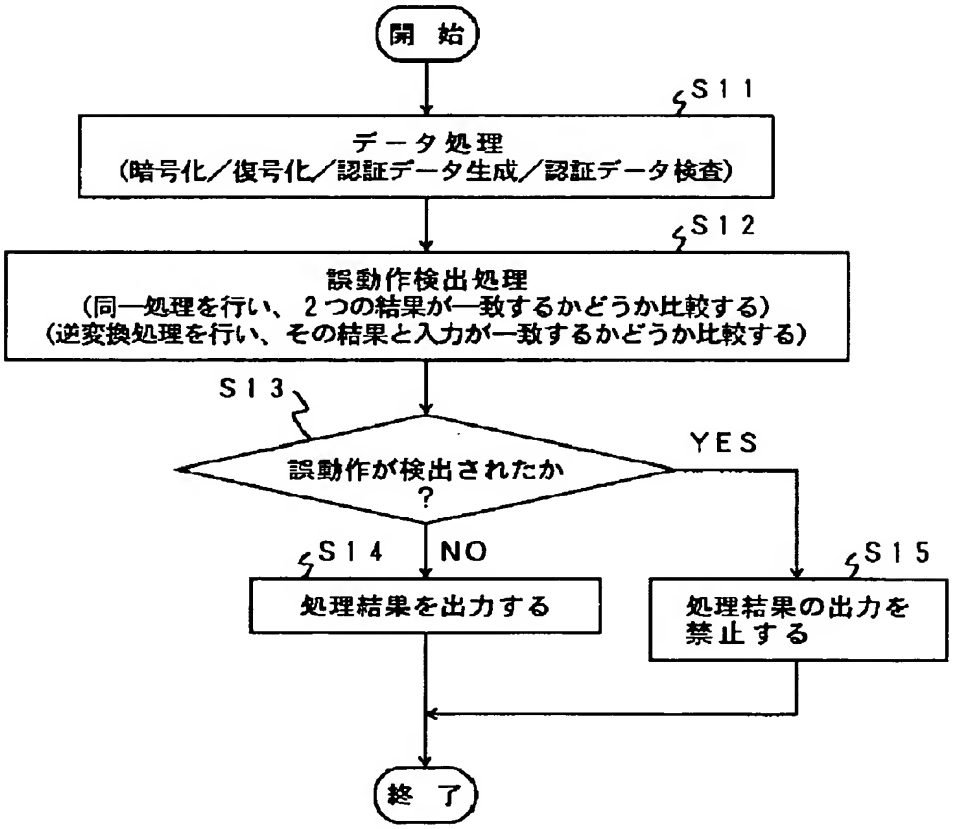
【図１】


入力データ
S1 タンパーフリー装置
S2
データ処理部
S5
鍵保管部
S3
誤動作検出部
S4
出力制御部
出力データ

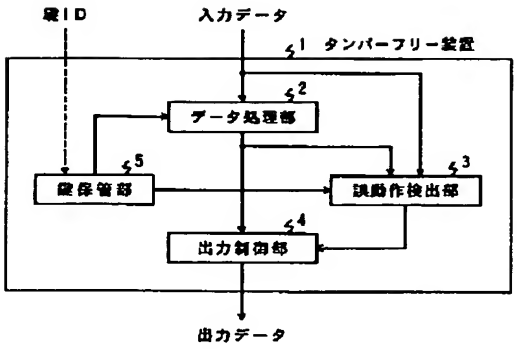
【図３】


入力データ
S1 タンパーフリー装置
S2
データ処理部
S5
鍵保管部
S3
誤動作検出部
S4
出力制御部
出力データ
制御情報

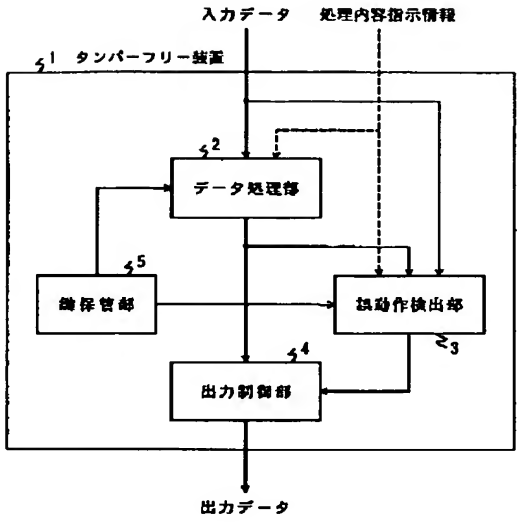
【図２】


開　始
S11
データ処理
(暗号化／復号化／認証データ生成／認証データ検査)
S12
誤動作検出処理
(同一処理を行い、２つの結果が一致するかどうか比較する)
(逆変換処理を行い、その結果と入力が一致するかどうか比較する)
S13
誤動作が検出されたか
？
YES
NO
S14
処理結果を出力する
S15
処理結果の出力を
禁止する
終　了

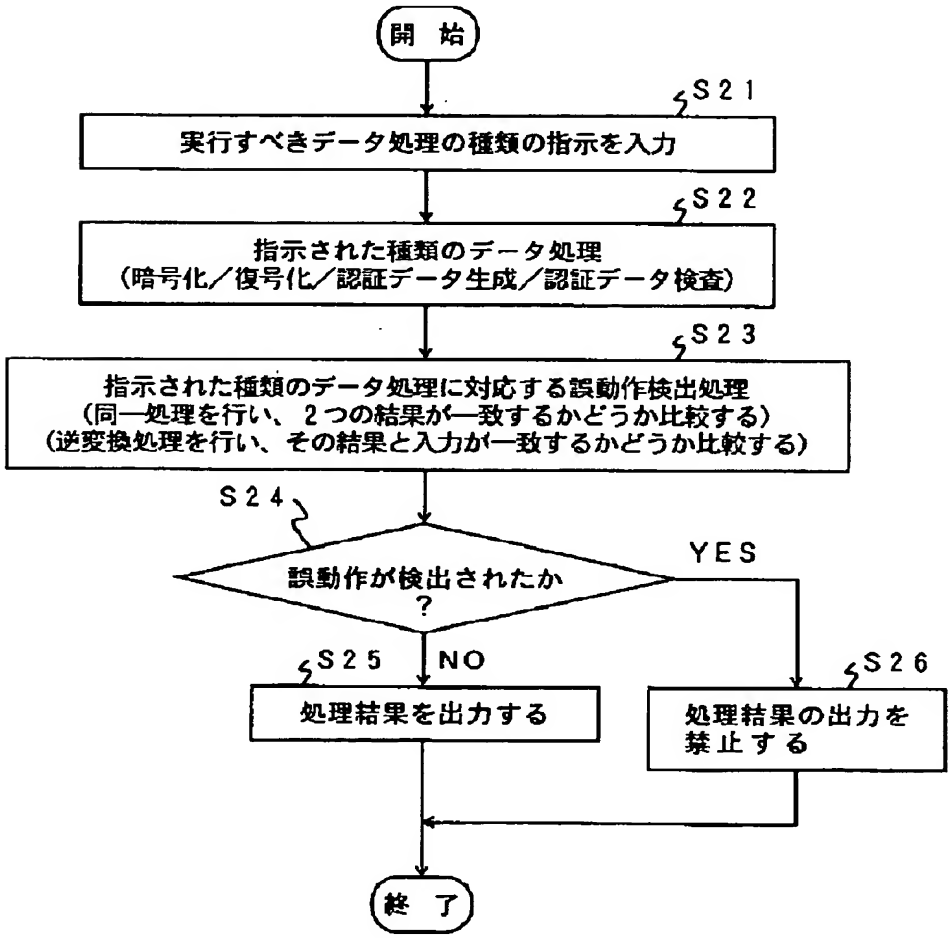
【図４】


鍵ID
入力データ
1 タンパーフリー装置
2 データ処理部
5 鍵保管部
3 誤動作検出部
4 出力制御部
出力データ

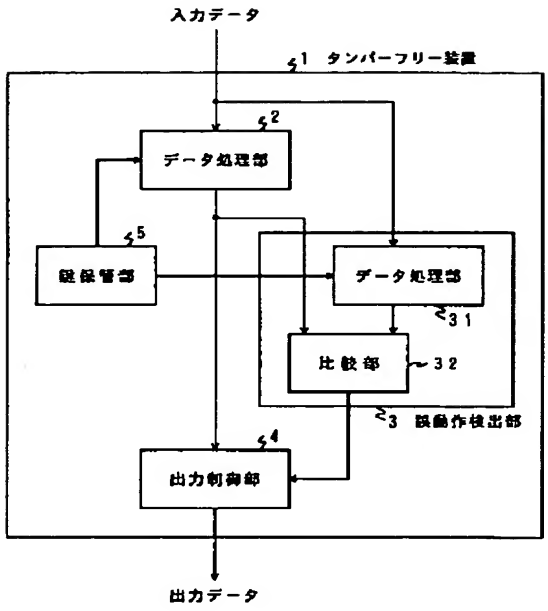
【図５】


入力データ
処理内容指示情報
1 タンパーフリー装置
2 データ処理部
5 鍵保管部
3 誤動作検出部
4 出力制御部
出力データ

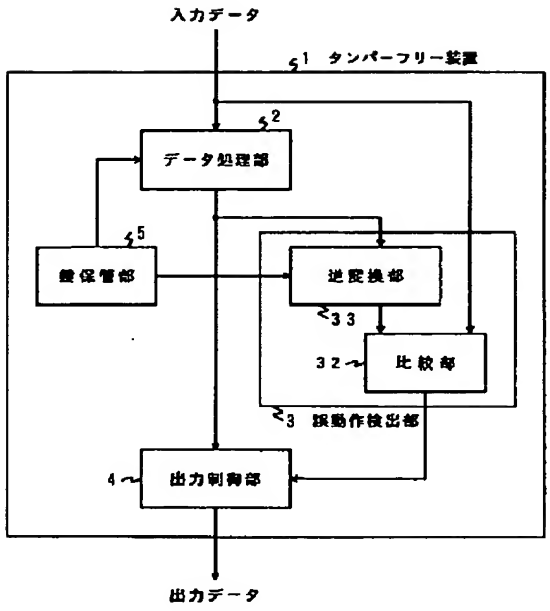
【図６】


開　始
S21
実行すべきデータ処理の種類の指示を入力
S22
指示された種類のデータ処理
（暗号化／復号化／認証データ生成／認証データ検査）
S23
指示された種類のデータ処理に対応する誤動作検出処理
（同一処理を行い、２つの結果が一致するかどうか比較する）
（逆変換処理を行い、その結果と入力が一致するかどうか比較する）
S24
誤動作が検出されたか
？
YES
NO
S25
処理結果を出力する
S26
処理結果の出力を
禁止する
終　了

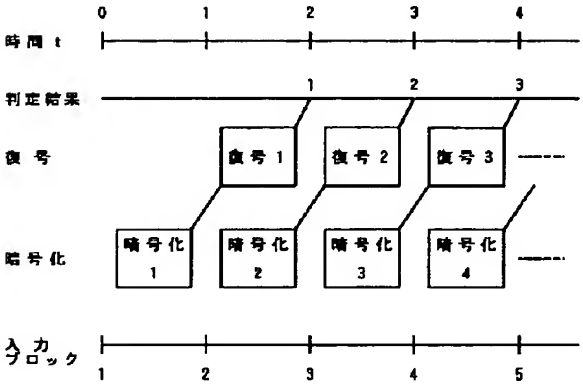
【図７】


入力データ
1 タンパーフリー装置
2
データ処理部
5
鍵保管部
データ処理部
31
比較部
32
3 誤動作検出部
4
出力制御部
出力データ

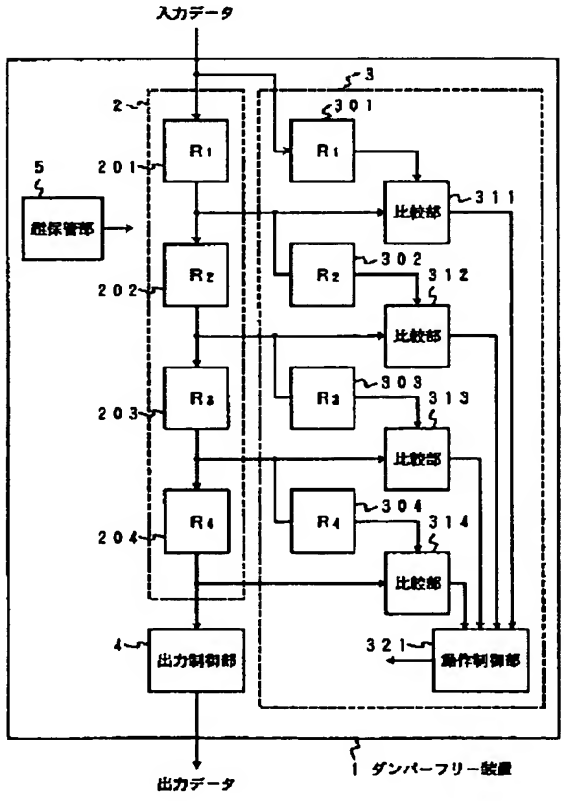
【図８】


入力データ
1 タンパーフリー装置
2
データ処理部
5
鍵保管部
逆変換部
33
32
比較部
3 誤動作検出部
4
出力制御部
出力データ

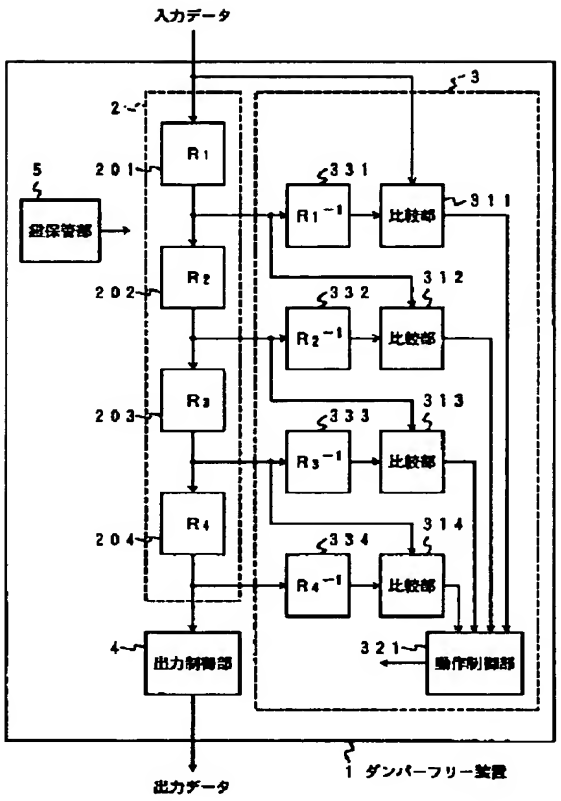
【図９】


0
1
2
3
4
時間 t
判定結果
1
2
3
復号
復号 1
復号 2
復号 3
暗号化
暗号化 1
暗号化 2
暗号化 3
暗号化 4
入力ブロック
1
2
3
4
5

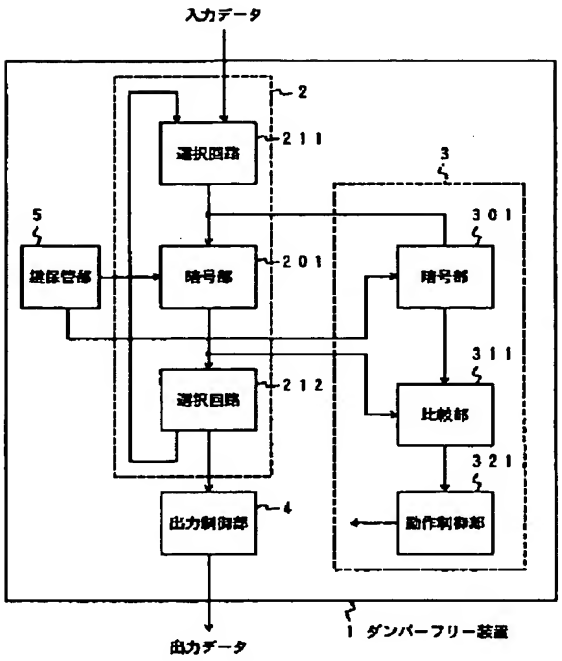
【図１０】


入力データ
3
301
2
R1
201
5
鍵保管部
311
比較部
R2
302
312
202
R3
303
313
203
R4
304
314
204
4
出力制御部
321
動作制御部
1 タンパーフリー装置
出力データ

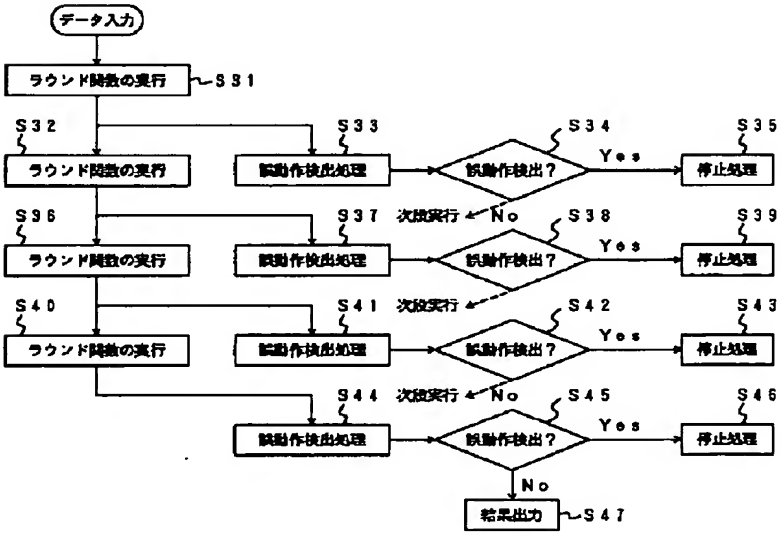
【図１１】


入力データ
3
2
5
201
R1
331
R1⁻¹
比較部
311
鍵保管部
R2
202
332
312
R2⁻¹
比較部
R3
203
333
313
R3⁻¹
比較部
R4
204
334
314
R4⁻¹
比較部
4
出力制御部
321
動作制御部
出力データ
1 ダンパーフリー装置

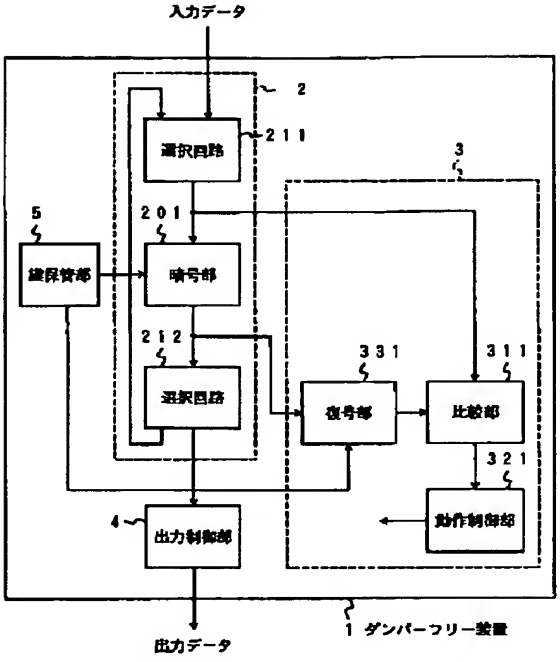
【図１３】


入力データ
2
211
選択回路
3
5
301
鍵保管部
暗号部
201
暗号部
311
212
選択回路
比較部
321
4
出力制御部
動作制御部
出力データ
1 ダンパーフリー装置

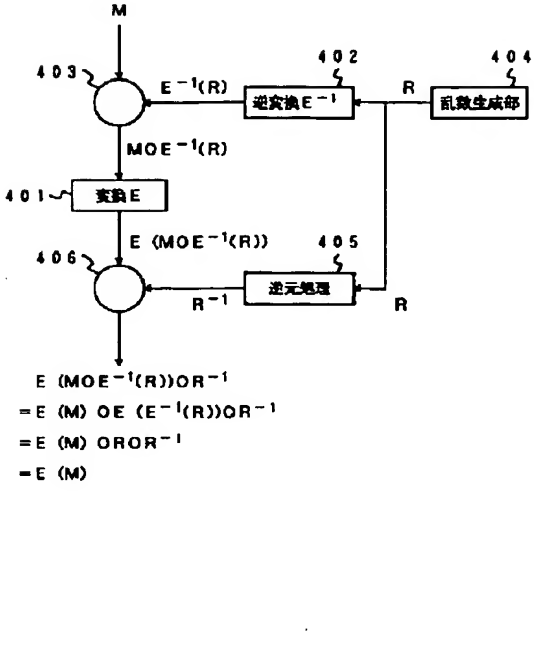
【図１２】


データ入力
ラウンド関数の実行
S31
S32
S33
S34
S35
ラウンド関数の実行
誤動作検出処理
誤動作検出？
Yes
停止処理
S36
S37
次段実行
No
S38
S39
ラウンド関数の実行
誤動作検出処理
誤動作検出？
Yes
停止処理
S40
S41
次段実行
S42
S43
ラウンド関数の実行
誤動作検出処理
誤動作検出？
Yes
停止処理
S44
次段実行
No
S45
S46
誤動作検出処理
誤動作検出？
Yes
停止処理
No
結果出力
S47

【図１４】


入力データ
2
選択回路
211
3
5
201
暗号部
鍵保管部
212
選択回路
331
311
復号部
比較部
321
4
出力制御部
動作制御部
出力データ
1 ダンパーフリー装置

【図１６】


M
403
E⁻¹(R)
402
逆変換E⁻¹
R
404
乱数生成部
MOE⁻¹(R)
401
変換E
E (MOE⁻¹(R))
406
405
逆元処理
R⁻¹
R
E (MOE⁻¹(R))OR⁻¹
=E (M) OE (E⁻¹(R))OR⁻¹
=E (M) ORR⁻¹
=E (M)